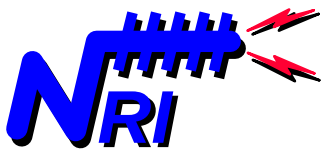
C^3 SCADA Server
Computer System Maintenance Procedures
Telemetry And Control System Engineering Series

Version 1.04 - Owner
20 Dec 2010



Navionics Research, Inc.
Saint Louis, Missouri USA
wireless-telemetry.com

TABLE OF CONTENTS

1 INTRODUCTION

In 1995, Navionics Research introduced the **WiSTAR** Network, an acronym derived from **Wi**reless **S**ystem **T**elemetry **A**nd **R**emote-Control. This product was designed to solve the problems posed by the complex distributed control and monitoring requirements of the rural water and wastewater industries.

During the early design of the WiSTAR Telemetry System, tools were added to the C^3 Computer to enable remote access to the telemetry system – enabling the Operators, Navionics Research, and the Consulting Engineers to study past history and perform upgrades, diagnostic procedures, and troubleshooting from great distances.

The first remote access was accomplished via Microsoft's "Dialup Networking Server" contained in Windows95 and above (The Microsoft "Plus Pack" was required for Windows95.) Personnel could connect to the Telemetry System via a remote, modem-equipped computer (but only one person at a time). An installation of Navionics Research software was also required on the remote computer.

However, with the growth of the internet and internet-related software technologies, Navionics Research set a goal of providing secure remote access through the internet. Because the networking software that accompanies Microsoft Windows is leveraged to the fullest extent, only internet web browser software would be required on the remote computer (included with all modern computer operating systems), and multiple personnel could connect simultaneously. A further benefit is that an extremely remote user need not incur long-distance telephone charges if a local internet access telephone number is available.

However, because the SCADA C^3 Computer is connected to the internet with a dedicated line (telephone, cable, DSL, or wireless internet), special attention to security maintenance is required.

For example, security flaws are occasionally discovered in the Microsoft Windows operating system. After such a flaw is discovered, Microsoft typically releases a free patch that can be downloaded from the "Windows Update" website. However, within months of the discovery of a security flaw, computer crackers often produce a "virus" or "worm" capable of exploiting the vulnerability. For this reason, it is imperative that the system's security be maintained at regular, frequent intervals.

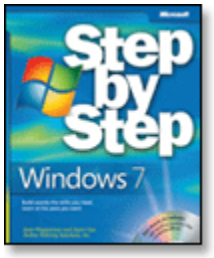
By visiting the Windows Update website on a frequent and regular basis, and by installing the recommended patches, computer owners can be assured that their system is protected from known security flaws.

The purpose of this tutorial is to provide assistance to operators who wish to keep their C^3 Computer system's security up-to-date. Each chapter focuses on a specific task, and detailed sequential procedures are given to accomplish this task.

The procedures taught in this manual were determined through years of experience and observation of working Navionics Research SCADA Systems at several client locations.

Intermediate computer experience is required of the reader. If the reader does not have the minimum experience required, then the following book is recommended before proceeding further:

Microsoft Windows 7 Step by Step



Description:
http://www.microsoft.com/learning/en/us/Book.aspx?ID=13485&locale=en-us

Buy Online:
www.amazon.com

2 THE 10 COMMANDMENTS OF SCADA SECURITY

1. DO NOT USE THE SCADA C^3 COMPUTER FOR NON-SCADA PURPOSES!

Including – but no limited to – email, web surfing, word processing, business software, billing software, games, instant messaging, internet chat, music sharing, etc. In other words – anything else besides the installed SCADA software. Often, the addition of 3rd party software introduces new security problems into a system. If other uses for the computer are required, then it is advised that another computer be purchased for those purposes. If non-SCADA software is used, then the risk of security breach increases dramatically.

2. INSTALL THE FREE SECURITY UPDATES FROM MICROSOFT FREQUENTLY AND REGULARLY.

As security flaws are discovered within the Microsoft Windows operating system, free patches are released that eliminate these flaws. By checking Microsoft's "Windows Update" website regularly and frequently, and by installing the recommended patches, the system will be kept up-to-date and will be more secure.

3. DO NOT INSTALL 3RD PARTY SOFTWARE ON THE COMPUTER; AND DO NOT ADD EXTRA HARDWARE TO THE COMPUTER.

Each C^3 computer has been carefully outfitted, with both hardware and software, for the specified SCADA tasks. The addition of extra software and hardware (and the hardware's associated driver software) can make the system less secure. If the use of 3rd party software or extra hardware is required, then install and use the extra hardware/software on another computer.

4. NEVER REVEAL A USERNAME/PASSWORD PAIR TO ANOTHER PERSON.

If another person requires access to the SCADA system, but does not have a username/password pair installed on the SCADA system – then do not provide him/her with the username/password for another person. A new and separate username/password for this individual should be provided and programmed into the system. If an operator shares his username/password with someone else, then all of the other person's actions will be logged under the actions of the operator. In other words, the operator will become responsible for the actions of this new user; and the security audit trail breaks down.

Anyone who attempts to gain access without Water Company approval (i.e. by asking to "borrow" another user's username/password pair) should be viewed with suspicion. Report any suspicious attempts or requests to the Water Company manager immediately.

5. IF A USERNAME/PASSWORD PAIR IS SUSPECTED TO HAVE BEEN COMPROMISED, OR IF AN EMPLOYEE WHO HAD ACCESS TO THE SYSTEM IS TERMINATED – THEN DELETE HIS/HER USERNAME/PASSWORD FROM THE SYSTEM IMMEDIATELY... AND UNTIL THIS ACTION IS TAKEN, DISCONNECT THE SCADA SYSTEM FROM THE INTERNET OR TELEPHONE LINE IMMEDIATELY.

Username/password pairs are like "keys" to the water treatment plant. In the wrong hands, malicious actions can be taken to disrupt the operation of the water treatment and distribution system. Therefore, treat all possible compromises of username/password pairs as serious vulnerabilities that must be corrected immediately.

6. DO NOT ADD EXTRA WINDOWS USER ACCOUNTS TO THE SYSTEM.

The computer has been set up with three (3) accounts: Operator, Navionics Research, and Administrator. No other accounts are necessary, and the addition of extra user accounts may compromise the security of the system. Also, do not modify the permissions of the existing accounts. These permission settings have been chosen for optimal security.

7. ONLY PROVIDE SCADA SYSTEM ACCESS TO PERSONNEL WHOSE JOB REQUIRES IT. AND ONLY PROVIDE THE MINIMUM FUNCTIONALITY THAT EACH PERSON REQUIRES.

The telemetry system's remote access server is certainly interesting, and typically many people associated with the Water Company desire access to view the status of the system. However, if it's not necessary for an individual to have access to the SCADA system – then don't provide it to him/her. Extra users increases the possibility that a username/password can become compromised.

8. REGULARLY REVIEW THE ACCESS LOGS.

The SCADA System has access logs that can be viewed by the operator. It is recommended that each of these logs be reviewed periodically and compared against known user access. If any suspicious activity is encountered in the log files, then disconnect the system from the internet or phone line until the security of the system is verified.

9. IF UNCERTAIN, CALL NAVIONICS RESEARCH FOR A CONSULTATION.

Do not hesitate to ask for advice from Navionics Research. If there is uncertainty regarding any security-related topic – call Navionics Research toll-free (888)993-3554.

10. IF THE PROPER SECURITY PROCEDURES ARE NOT BEING FOLLOWED, THEN DISCONNECT THE COMPUTER FROM THE INTERNET OR TELEPHONE LINE.

This manual includes procedures that must be performed regularly in order to maintain high security within the SCADA System. If the regular maintenance becomes too burdensome, or if new personnel are hired and not properly trained – then disconnect the system from the internet or telephone line. To keep a non-maintained system online is to simply invite security problems. Rather than suffer a security breach, it would be better to simply disconnect from the internet or telephone line and thereby disable the remote access features altogether.

3 WINDOWS UPDATE

Occasionally, security flaws are discovered in the Microsoft Windows operating system. After such a flaw is discovered, Microsoft typically releases a free patch that can be downloaded from the "Windows Update" website. However, within months of the discovery of a security flaw, computer crackers often produce a "virus" or "worm" capable of exploiting the vulnerability. For this reason, it is imperative that the system's security be maintained at regular, frequent intervals.

By visiting the Windows Update website on a frequent and regular basis, and by installing the recommended patches, computer owners can be assured that their system is protected from known security flaws.

1. To run "Windows Update", first log on to the C^3 computer under the "Navionics Research" account, thereby garnering the "Administrator" privileges that are required to complete this procedure.

2. Left-click on "Start" > "Programs" > "Windows Update".

3. Follow the prompts to install the critical updates. It has been observed on occasion that the installation of several (>3) patches simultaneously can cause the system to "hang" or "lock up". Therefore, it is recommended that only 3 or fewer patches be installed at any given attempt.

4. Usually, after the installation of critical update(s), the user is prompted to restart the computer. This step is normal and should be performed as requested.

5. After running Windows Update, and after performing the restart (if required), return to Step #1 and re-run Windows Update. When Windows Update reports that there are no further patches to install, then the procedure is completed.

6. When the procedure is completed, then log out of the "Navionics Research" account, and log in to the "Operator" account to resume SCADA operations.

7. If further information is desired, refer to the recommended reading:

"Microsoft Windows 7 Step by Step".

Or refer to the official "Windows Update" website:

http://windowsupdate.microsoft.com

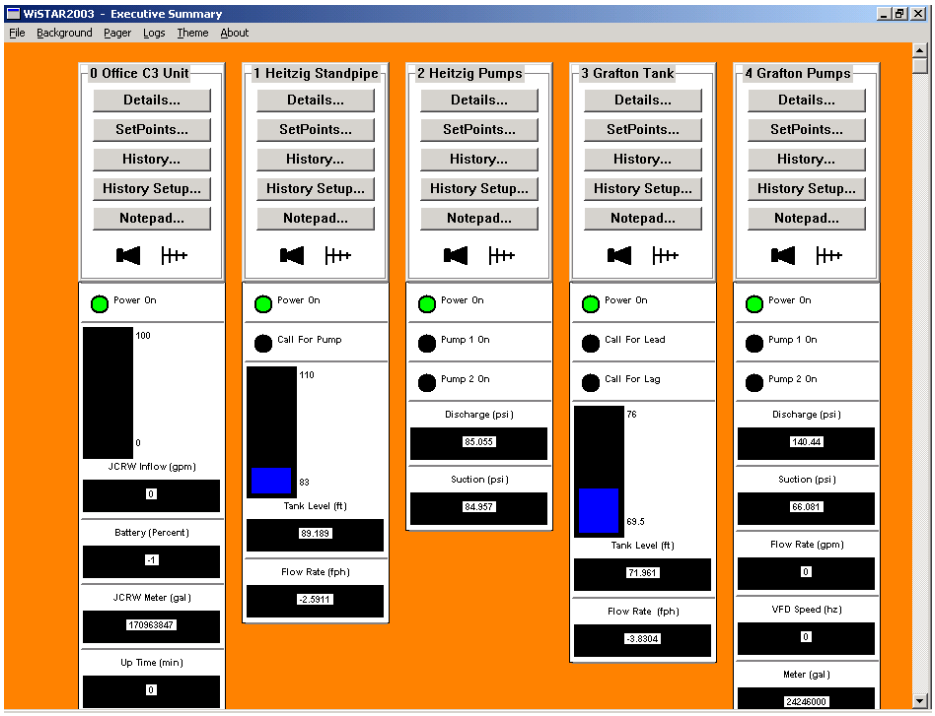
4 REVIEWING THE LOG FILES

An audit trail of log files is maintained by the security subsystem of the SCADA System. The following log files are included:

A. Review NRI Access Log –

i. Consists of a descriptive log file that details every web page request and action. The full URL is listed, along with the username and IP address of the remote user is included.

ii. Available through the WiSTAR-Executive Summary Main Menu.



B. Review Web Server Access Log –

i. Consists of an access log file that is maintained by the Web Server Software.

ii. Available through the Apache Group Folder:
Start > Programs > Apache Group > Server Logs > Access Log

C. Review Web Server Error Log –

i. Consists of an error log file that is maintained by the Web Server Software.

ii. Available through the Apache Group Folder:
Start > Programs > Apache Group > Server Logs > Error Log

5 ADDING AND DELETING A WEB ACCESS ACCOUNT

ADDING A WEB ACCESS ACCOUNT:

A. Left-click: Start > Programs > Apache Group > Configure Web Server > Edit Web Configuration File

B. On the line that contains the valid usernames, add the new username.

C. Save the file and exit.

D. Edit the password file by adding a line containing the new username and password separated by a colon (:).

The password file is located at:

\Program Files\Apache Group\Apache 2\access.txt

E. Stop the web server and re-start the web server.

DELETING A WEB ACCESS ACCOUNT:

A. Left-click: Start > Programs > Apache Group > Configure Web Server > Edit Web Configuration File

B. On the line that contains the valid usernames, delete the desired username.

C. Save the file and exit.

D. Edit the password file by deleting the line containing the relevant username and password.

The password file is located at:

\Program Files\Apache Group\Apache 2\access.txt

E. Stop the web server and re-start the web server.

6 CHANGING PASSWORD(S) FOR A WEB ACCESS ACCOUNT

A. Edit the password file by modifying the line containing the relevant username and password. The username / password pair is contained on a single line and separated by a colon (:). The format is as follows:

username:password

The password file is located at:

\Program Files\Apache Group\Apache 2\access.txt

B. Stop the web server and re-start the web server.

7 SETTING/CHANGING PERMISSIONS FOR A WEB ACCESS ACCOUNT

A. Each RTU or C^3 location has a unique address between 0 and 255. And a permission description file for each site exists within the security subsystem.

The permission files are located within the following directory:

\wistar\sys01\realtime\

The filenames are formed with the following format:

auth.nnn

where nnn is the address. For example, the file containing permission information for site #0 is “auth.000”.

B. A typical permission file is shown below:

```
johnsmiththeoperator:manager
scadamfgr:manager
systemintegrator:manager
engineer:guest
employee1name:setpoint
employee2name:alarm
secretaryname:guest
```

C. Notice that the username precedes the permission level, separated by a colon (:). The permission levels are described as follows:

manager:	everything allowed.
operator:	everything allowed, except modification of permissions.
user:	everything allowed, except modification of permissions, logs, troubleshooting, and pager numbers.
setpoint:	Same as “user”, except not allowed to modify alarms.
alarm:	Same as “user”, except not allowed to modify setpoints.
guest:	Same as “user”, except not allowed to modify alarms and setpoints.

This Page Intentionally Blank.